ABSTRACT

All execution paths of one or more assemblies in managed code are simulated to find the permissions for each execution path. The managed code can correspond to a managed shared library or a managed application. Each call in each execution path has a corresponding permissions set. When the library or application has permissions to execute that are not less than the required permission sets for the execution paths, any dynamic execution of the library or application will not trigger a security exception. The simulated execution provides a tool that can be used to ensure that code being written will not exceed a maximum security permission for the code. A permission set can be determined by the tool for each assembly corresponding to an application and for each entry point corresponding to a shared library.